APPARATUS AND METHOD FOR MONITORING NETWORK

Patent Number: JP2002064492

Publication date: 2002-02-28

Inventor(s): OKADA HISASHI; HIROTA YOICHI; YAMAGISHI NORIKAZU; TAKESADA MUTSUHARU

Applicant(s): HITACHI ELECTRONICS SERVICE CO LTD

Requested Patent: ⌐ JP2002064492

Application Number: JP20000247859 20000817

Priority Number(s):

IPC Classification: H04L12/24; H04L12/26; H04L12/28; H04L12/56; H04L29/14

EC Classification:

Equivalents:

Abstract

PROBLEM TO BE SOLVED: To provide a network monitor in which update of data is stopped depending on the data being taken in.
SOLUTION: A network monitoring computer 6 comprises a section 121 for taking in a packet on a network, and a section 122 for holding the packet. A data deciding section 14 makes a decision whether a packet acquired at the packet acquiring section 121 contains an IP address stored at an IP address storing section 13 and allotted to the network monitoring computer 6 or not. If that packet contains the IP address, a data acquisition control section 16 controls the operation such that packets being taken in subsequently are not written over a data storing section 122 and a communication control section 61 delivers Ping to other network monitoring computer stored at the IP address storing section 13.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－64492
（P2002－64492A）
(43)公開日　平成14年２月28日(2002.2.28)

(51)Int.Cl.[7]	識別記号	FI		テーマコード(参考)
Ｈ０４Ｌ 12/24		Ｈ０４Ｌ 11/08		５Ｋ０３０
12/26		11/00	３１０Ｚ	５Ｋ０３３
12/28		11/20	１０２Ｚ	５Ｋ０３５
12/56		13/00	３１３	
29/14				

審査請求　有　請求項の数８　ＯＬ　（全９頁）

(21)出願番号　特願2000－247859(P2000－247859)

(22)出願日　平成12年８月17日(2000.8.17)

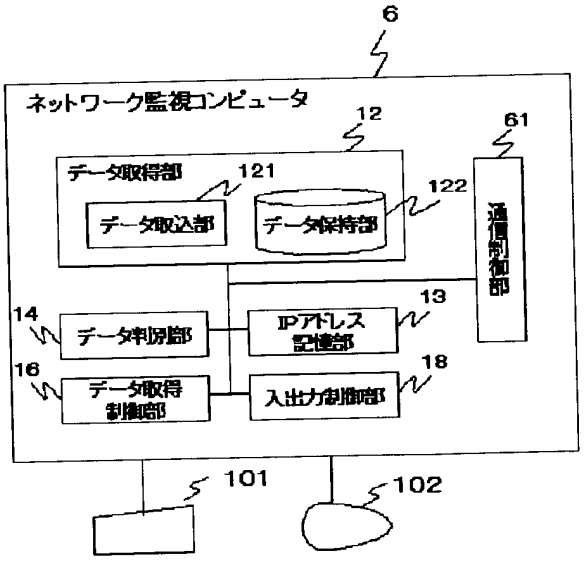
(71)出願人　000233491
日立電子サービス株式会社
神奈川県横浜市戸塚区品濃町504番地２
(72)発明者　岡田　尚志
神奈川県横浜市戸塚区品濃町504番地２
日立電子サービス株式会社内
(72)発明者　廣田　陽一
神奈川県横浜市戸塚区品濃町504番地２
日立電子サービス株式会社内
(74)代理人　100087170
弁理士　富田　和子　（外１名）

最終頁に続く

(54)【発明の名称】　ネットワーク監視装置および方法

(57)【要約】
【課題】　取り込んだデータに応じてデータの更新を停止するネットワーク監視装置の提供。
【解決手段】　ネットワーク監視コンピュータ６は、ネットワーク上のパケットを取り込むデータ取込部１２１と、パケットを保持するパケット保持部１２２とを備える。データ判別部１４が、パケット取得部１２１が取り込んだパケットがＩＰアドレス記憶部１３に記憶されたネットワーク監視コンピュータ６に割り振れられたＩＰアドレスを含むかどうかを判別する。取り込んだパケットに前記ＩＰアドレスが含まれる場合、データ取得制御部１６はそれ以降に取り込むパケットをデータ保持部１２２に上書きしないように制御し、通信制御部６１がＩＰアドレス記憶部１３に記憶された他のネットワーク監視コンピュータにＰｉｎｇを送る。

図6



【特許請求の範囲】
【請求項１】　複数の情報処理装置が接続されたネットワークの監視を行うネットワーク監視装置において、
前記ネットワークと接続されているときに、送信先装置の識別情報を少なくとも含む当該ネットワーク上のパケットを取り込んで、保持するパケット取得部と、
当該ネットワーク監視装置を識別するための識別情報を記憶する記憶領域を有する識別情報記憶部と、
前記パケット取得部が取り込んだパケットに含まれる前記送信先装置の識別情報が、前記識別情報記憶部に記憶された前記識別情報と一致するかどうかを判別する判別部と、
前記判別部における判別の結果、前記送信先装置の識別情報と前記識別情報記憶部に記憶された前記識別情報とが一致する場合、前記パケット取得部が前記パケットより後のパケットを保持しないように制御する制御部と、
を備えることを特徴とするネットワーク監視装置。
【請求項２】　請求項１記載のネットワーク監視装置において、
前記パケット取得部は、
前記パケットを前記ネットワークから取り込む取り込み部と、
前記取り込部が取り込んだパケットを保持する保持部と、を備え、
前記判別部における判別の結果、前記送信先装置の識別情報と前記識別情報記憶部に記憶された前記識別情報とが一致する場合、
前記制御部は、
前記取り込み部に前記パケットより後のパケットの取り込みを停止させることを特徴とするネットワーク監視装置。
【請求項３】　請求項１記載のネットワーク監視装置において、
前記パケット取得部は、
パケットを保持する保持部と、
前記パケットを前記ネットワークから取り込んで、前記保持部に書き込む取り込み部と、を備え、
前記制御部は、
前記判別部における判別の結果、前記送信先装置の識別情報と前記識別情報記憶部に記憶された前記識別情報とが一致する場合、
前記制御部は、
前記取り込み部が取り込んだ、前記パケットより後のパケットの前記保持部への書き込みを停止させることを特徴とするネットワーク監視装置。
【請求項４】　請求項１から３のうちのいずれか一項に記載のネットワーク監視装置において、
前記識別情報記憶部は、
他のネットワーク監視装置の識別情報を記憶する記憶領域をさらに有し、
当該ネットワーク監視装置は、
前記判別部における判別の結果、前記送信先装置の識別情報と前記識別情報記憶部に記憶された前記識別情報とが一致する場合、前記識別情報記憶部を参照して、前記他のネットワーク監視装置の識別情報を送信先装置の識別情報に設定したパケットを生成するパケット生成部と、
前記パケット生成部が生成したパケットを、前記ネットワークへ出力する出力部とを、さらに備えることを特徴とするネットワーク監視装置。
【請求項５】　請求項１から４のうちのいずれか一項に記載のネットワーク監視装置であって、
前記ネットワークの通信プロトコルは、ＴＣＰ／ＩＰであり、
前記ネットワーク上のパケットは、
少なくとも、当該パケットの送信先装置のＩＰアドレスを含み、
前記特定のパケットは、
当該パケットの送信先装置のＩＰアドレスに、特定のＩＰアドレスが設定されたｐｉｎｇコマンドのパケットであることを特徴とするネットワーク監視装置。
【請求項６】　複数の情報処理装置が接続されたネットワークと接続可能な情報処理装置において、
前記ネットワークと接続するための接続部と、
前記接続部が前記ネットワークと接続されているときに、送信先装置の識別情報を少なくとも含む当該ネットワーク上のパケットを取り込んで、保持するパケット取得部と、
当該情報処理装置を識別するための識別情報を記憶する記憶領域を有する識別情報記憶部と、
前記パケット取得部が取得したパケットに含まれる前記送信先装置の識別情報が、前記識別情報記憶部に記憶された前記識別情報と一致するかどうかを判別する判別部と、
前記判別部における判別の結果に応じて、当該パケットにより定まる情報に基づく処理を行う処理部と、
前記処理部が行う処理に伴って生じるエラーを検出するエラー検出部と、
前記エラー検出部がエラーを検出したとき、前記パケット取得部が前記パケットより後のパケットを保持しないように制御する制御部と、を備えることを特徴とする情報処理装置。
【請求項７】　記憶部を有するネットワーク監視装置におけるネットワーク監視方法であって、
当該ネットワーク監視装置を識別するための識別情報を前記記憶部に記憶し、
ネットワーク上のパケットを取り込み、前記記憶部に記憶されている識別情報が、当該取り込んだパケットに含まれるかどうかを判別し、
判別の結果、前記識別情報が前記パケットに含まれない

場合、前記取り込んだパケットを保持し、
判別の結果、前記識別情報が前記パケットに含まれる場合、前記パケットより後のパケットは保持しないことを特徴とするネットワーク監視方法。
【請求項８】　記憶部を有するネットワーク監視装置に実行させるプログラムを記録した記録媒体であって、
前記プログラムは、
当該ネットワーク監視装置を識別するための識別情報を前記記憶部に記憶する処理と、
ネットワーク上のパケットを取り込み、前記記憶部に記憶されている識別情報が、当該取り込んだパケットに含まれるかどうかを判別する処理と、
判別の結果、前記識別情報が前記パケットに含まれない場合、前記取り込んだパケットを保持する処理と、
判別の結果、前記識別情報が前記パケットに含まれる場合、前記パケットより後のパケットは保持しないように制御する処理と、
を前記ネットワーク監視装置に実行させることを特徴とする記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ネットワーク監視技術にかかり、特にネットワークからのパケットの取り込みを制御する技術に関する。
【０００２】
【従来の技術】ネットワークトラブルの原因を解析するために、ネットワーク上のパケットを取り込んで、取り込んだパケットを保持するＬＡＮアナライザが広く用いられている。このパケットを保持するための記憶領域は容量が限られているので、サイクリックに利用される。したがって、一定時間が経過すると取り込んだパケットであっても上書きされて、消失する。
【０００３】また、従来のＬＡＮアナライザでは、例えば、プロトコルにＴＣＰ／ＩＰを採用しているネットワークであれば、物理層、データリンク層、ネットワーク層、トランスポート層、セッション層でのプロトコルエラーを検出することができる。このエラーを検出すると、データの取得を停止して、その時点で記憶領域に保持されているデータが消失しないようにするストップトリガー機能がある。
【０００４】
【発明が解決しようとする課題】しかしながら、通信の過程に原因があった場合でも、アプリケーション層などのデータにエラーが発生すると、ＬＡＮアナライザはそのエラーを認識することができない。そのため、アプリケーション層などでのエラーを検出してストップトリガーをかけることもできない。したがって、この場合は、エラー発生時点の記憶領域のデータを保持し続けることが出来ないという問題点があった。
【０００５】本発明は、このような従来の問題点に着目し、取り込んだデータに応じてデータの更新を停止するネットワーク監視技術を提供することを目的とする。
【０００６】
【課題を解決するための手段】前記目的を達成するため、本発明では識別情報を記憶する記憶部を備えたネットワーク監視装置が、以下の処理を行う。すなわち、当該ネットワーク監視装置を識別するための識別情報を記憶部に記憶する。ネットワーク上のパケットを取り込み、前記記憶部に記憶されている識別情報が、当該取り込んだパケットに含まれるかどうかを判別する。前記識別情報が前記パケットに含まれない場合、前記取り込んだパケットを保持する。前記識別情報が前記パケットに含まれる場合、前記パケットより後のパケットは保持しない。
【０００７】
【発明の実施の形態】以下、本発明の実施形態について、図面を用いて説明する。
【０００８】図１は、第１の実施形態が適用されるネットワークシステムの全体構成図である。すなわち、ネットワーク監視装置であるＬＡＮアナライザ１ａ，１ｂと、コンピュータ２ａ，２ｂと、テスト用コンピュータ３ａ，３ｂと、がＬＡＮ（Local Area Network）８ａ，８ｂに接続されている。それぞれ同一構成のＬＡＮ８ａ，８ｂがＷＡＮ（Wide Area Network）９で接続されている。このネットワークシステムは、通信プロトコルにＴＣＰ/ＩＰを用いている。ただし、通信プロトコルはＴＣＰ/ＩＰに限定されない。たとえば、他の通信プロトコルを用いてもよいし、ＩＰ（インターネットプロトコル）と、ＴＣＰ（トランスミッションコントロールプロトコル）以外の上位プロトコルとを組み合わせてもよい。
【０００９】本実施の形態では、コンピュータ２ａ、２ｂが、あらかじめ定められた事象の発生を検出して、それをＬＡＮアナライザ１ａ、１ｂが検知可能な事象に変換を行う。具体的には、コンピュータ２ａ、２ｂが、アプリケーション層でのエラー等を検出すると、ネットワーク上にあるすべてのコンピュータにとって、論理的に存在しないＩＰアドレス（新規に割り当てられたＩＰアドレス）に対するｐｉｎｇコマンドの発行という事象に変換する。
【００１０】ＬＡＮアナライザ１は、ネットワークのトラブル発生時等に設置され、ＬＡＮ８上のパケットを取り込んで保持する。ネットワークの保守担当者は、ＬＡＮアナライザに保持されたパケットを解析して、トラブルの原因の究明に役立てる。ＬＡＮアナライザ１の詳細な構成は図４（ａ）を用いて説明する。
【００１１】ＬＡＮアナライザ１は、図４（ａ）に示すように、キーボード等の入力装置１０１およびＣＲＴ、液晶ディスプレイ等の表示装置１０２が接続されている。ＬＡＮアナライザ１は、データ取得部１２と、ＩＰ

アドレス記憶部１３と、データ判別部１４と、データ取得制御部１６と、表示制御部１８とを、その内部機能として備える。これらの内部機能は、プロセッサが所定のプログラムを読み込んで、それを実行することにより実現される。

【００１２】データ取得部１２は、データ取込部１２１とデータ保持部１２２とを有する。データ取込部１２１は、ＬＡＮ上のパケットを取り込む。取り込んだパケットは、図示しないバッファに一時的に記憶される。

【００１３】データ保持部１２２は、データ取込部１２１が取り込んだパケットを保持する。データ保持部１２２は、例えば、一定の容量を持つサイクリックバッファで構成される。つまり、例えば１００メガバイト程度の容量を持ち、パケットを順次記憶していき、全領域にデータが記憶された状態になると、時間的に最も古いデータに上書きして記憶していく。

【００１４】ＩＰアドレス記憶部１３は、ＬＡＮアナライザ１と同じＬＡＮ８に接続されているテスト用コンピュータ３に設定されたＩＰアドレス８０を記憶する領域を備える。例えば、ＬＡＮアナライザ１ａのＩＰアドレス記憶部１３には、テスト用コンピュータ３ａのＩＰアドレス８０ｃ（***.***.34.56）が記憶される。

【００１５】データ判別部１４は、データ取込部１２が取り込んだパケットが特定のパケットであるかどうかを判別する。例えば、取り込んだパケットの送信先のＩＰアドレスがＩＰアドレス記憶部１３に記憶されているＩＰアドレスと一致するかどうかを判別する。具体的には、ＬＡＮアナライザ１ａでは、取り込んだパケットの送信先ＩＰアドレスが、ＩＰアドレス８０ｃ（***.***.34.56）であるかどうかを判別する。さらに好ましくは、取り込んだパケットがＰｉｎｇコマンドであるかどうかを併せて判別してもよい。

【００１６】判別の結果、特定のパケットである場合は、その旨をデータ取得制御部１６へ通知する。特定のパケットでない場合は、データ取込部１２１に対して、図示しないバッファに記憶されているパケットをデータ保持部１２２へ書き込むように指示する。

【００１７】データ取得制御部１６は、データ取得部１２が行うデータ取得を制御する。例えば、データ判別部１４からの通知を受けて、データ取得部１２に対して、特定のパケットより後のパケットを保持しないように指示する。好ましくは、前記特定のパケットより後にＬＡＮ上を伝送されてくるパケットについては、データ取込部１２１が取り込まないように制限するようにしてもよい。あるいは、前記特定のパケットより後にＬＡＮ上を伝送されてきて、データ取込部１２１が取り込んだパケットについては、図示しないバッファからデータ保持部１２２へ書き込まないようにしてもよい。

【００１８】こうすることで、特定のパケットを受信した以降、データ保持部１２２の記憶内容が更新されて、書きかえられてしまうことを回避できる。その結果、特定のパケットを受信する直前にネットワーク上に存在したパケットが上書きされずに、保持しつづけることができる。

【００１９】入出力制御部１８は、入力装置１０１および表示装置１０２の制御を行う。例えば、入力装置１０１から入力を受け付け、表示装置１０２にデータ保持部１２２に保持しているデータを表示させる。

【００２０】コンピュータ２ａとコンピュータ２ｂには、それぞれＩＰアドレス８０ａ，８０ｂが割り振られていて、相互に通信を行い、所定のアプリケーションを実行する。コンピュータ２の詳細な構成は、図４（ｂ）を用いて説明する。図４（ｂ）に示すように、コンピュータ２は、通信制御部２１と、１以上のデータ処理部２２と、データ処理部２２でのエラー発生を検出するエラー検出部２３と、ＩＰアドレス記憶部２４を、その内部機能として備える。これらの内部機能は、プロセッサが所定のプログラムを読み込んで、それを実行することにより実現される。

【００２１】通信制御部２１は、ネットワーク上の他の装置との通信を制御する。例えば、ＬＡＮ８上のパケットを取得し、自コンピュータ２宛てのパケットを受け付ける。また、ネットワーク上の他の装置へ送信するために、パケットを生成して、ＬＡＮ８へ出力する。

【００２２】データ処理部２２は、通信制御部２１が受け付けたパケットが示す情報に基づいて、ユーザが定義した所定のアプリケーション処理を行う。

【００２３】エラー検出部２３は、データ処理部２２であらかじめ定められた事象が発生したかどうかを監視し、当該事象が発生すると、それをエラーとして検出する。エラー検出部２３が検出すべき事象は、ユーザが任意に指定することができる。たとえば、データ処理部２２における処理の異常終了、他の装置との通信処理におけるタイムアウト等の通信不良、プロトコルの上位階層でのエラー等を検出するようにしてもよい。さらに好ましくは、いわゆる警告のような軽微な不具合もエラーとして検出するようにしてもよい。

【００２４】さらに、エラー検出部２３は、エラーを検出すると、ＩＰアドレス記憶部２４に記憶されているＩＰアドレスの装置に対してエラー検出を通知する。例えば、ＩＰアドレス記憶部２４に記憶されているＩＰアドレスへ宛てて、Ｐｉｎｇコマンドを発行するように通信制御部２１へ指示する。

【００２５】ＩＰアドレス記憶部２４は、ＬＡＮアナライザ１と同じＬＡＮ８に接続されているテスト用コンピュータ３に設定されたＩＰアドレス８０、および、ＷＡＮ９を介して接続される他のＬＡＮ８に接続されているテスト用コンピュータ３に設定されたＩＰアドレス８０を記憶する。例えば、コンピュータ２ａ、２ｂのいずれのＩＰアドレス記憶部２４にも、テスト用コンピュータ

３ａ、３ｂのＩＰアドレス８０ｃ（***.***.34.56）および８０ｄ（***.***.12.78）が記憶される。

【００２６】テスト用コンピュータ３ａ，ｂは、ネットワークトラブルの解析用に設置されるコンピュータである。したがって、通常時には設置する必要はない。各テスト用コンピュータ３ａ，ｂには、それぞれＩＰアドレス８０ｃ、８０ｄが割り振られている。テスト用コンピュータ３は、ＩＰアドレスを割り振って、ＬＡＮ８に接続できる装置であれば、なんでもよい。

【００２７】本実施形態での処理手順について、図７を用いて説明する。

【００２８】図７は、ＬＡＮアナライザ１ａの処理手順を示したものである。ＬＡＮアナライザ１ｂについては、ＬＡＮ８ａとＬＡＮ８ｂが異なる点以外は同様である。

【００２９】入力装置１０１から所定の指示を受けて、データ取込１２１がデータの取り込みを開始する（Ｓ１０１）。取り込んだパケットがテスト用コンピュータ３ａ宛てのものであるかどうかを判別する（Ｓ１０２）。テスト用コンピュータ３ａ宛てでない場合には、そのパケットをデータ保持部１２２に書き込んで保持する（Ｓ１０３）。その後、Ｓ１０１へ戻って処理を繰り返す。これにより、コンピュータ２ａ，２ｂ間の通信を含む、ＬＡＮ８ａ上のパケットが保持されていく。

【００３０】このとき、例えば、コンピュータ２ｂのデータ処理部２２でエラーが発生したとする。すると、コンピュータ２ｂのエラー検出部２３がエラーを検出する。そして、コンピュータ２ｂからテスト用コンピュータ３ａ，３ｂに宛ててＰｉｎｇコマンドが発行される。

【００３１】ＬＡＮアナライザ１ａが、テスト用コンピュータ３ａ宛てのパケットを取り込むと（Ｓ１０１、Ｓ１０２）、データ取得制御部１６が、そのパケットより後にＬＡＮ８ａ上を伝送されてくるパケットの取得を禁止する（Ｓ１０４）。これにより、データ保持部１２２が更新されない。つまり、テスト用コンピュータ３ａ宛てのパケットを取得した時点でデータ保持部１２２に記憶されているパケットが、そのまま保持される。

【００３２】つぎに、本発明の第２の実施形態が適用されるネットワークシステムの全体構成図を図２に示す。すなわち、ネットワーク監視装置であるＬＡＮアナライザ１と、コンピュータ２と、テスト用コンピュータ３と、がＬＡＮ８に接続されている。監視コンピュータ５がＬＡＮ８ｂに接続され、ＬＡＮ８ａ，ｂがＷＡＮ９で接続されている。なお、以下の実施形態において、第１の実施形態と同一の構成には同一の符号を付して説明を省略する場合がある。

【００３３】本実施形態で用いるＬＡＮアナライザ１、コンピュータ２、テスト用コンピュータ３の構成は、第１の実施形態と同様である。

【００３４】監視コンピュータ５は、コンピュータ２の状態を監視する。監視コンピュータ５の構成は図５に示すように、通信制御部５１と、監視制御部５２と、ＩＰアドレス記憶部５３とを、その内部機能として備える。これらの内部機能は、プロセッサが所定のプログラムを読み込んで、それを実行することにより実現される。

【００３５】通信制御部５１は、ネットワーク上の他の装置との通信を制御する。例えば、ＬＡＮ８上のパケットを取得し、自監視コンピュータ５宛てのパケットを受け付ける。また、ネットワーク上の他の装置へ送信するために、パケットを生成して、ＬＡＮ８へ出力する。

【００３６】監視制御部５２は、コンピュータ２の動作状態を監視する。例えば、定期的にコンピュータ２に対してメッセージを出力し、応答があるかどうかを確認する。応答がない場合、コンピュータ２に何等かの異常があるとみなして、テスト用コンピュータ３へその旨を通知する。具体的には、定期的にコンピュータ２宛てのＰｉｎｇコマンドを出力するように通信制御部５１へ指示する。このＰｉｎｇに対する応答を通信制御部５１を介して受け付ける。一定時間内に応答がない場合、テスト用コンピュータ３へＰｉｎｇコマンドを出力するように通信制御部５１へ指示する。

【００３７】ＩＰアドレス記憶部５３は、少なくとも、コンピュータ２１と、テスト用コンピュータ３に設定されたＩＰアドレス８０ａ、８０ｃを記憶する。

【００３８】本実施形態における監視コンピュータ５の処理手順について説明する。ＬＡＮアナライザ１の処理手順は、図７と同様である。

【００３９】コンピュータ２が図示しない他の装置等と通信をしながら、所定の処理を行っている。このときに、監視コンピュータ５は、コンピュータ２に対して定期的にＰｉｎｇコマンドを送り、その応答を確認する（Ｓ２０１、Ｓ２０２）。所定時間内に応答がない場合等、異常を検出した場合、監視コンピュータ５はテスト用コンピュータ３へＰｉｎｇを発行する（Ｓ２０３）。

【００４０】このテスト用コンピュータ３宛てのＰｉｎｇを受け取ったＬＡＮアナライザ１は、図７のフローにしたがって動作する。

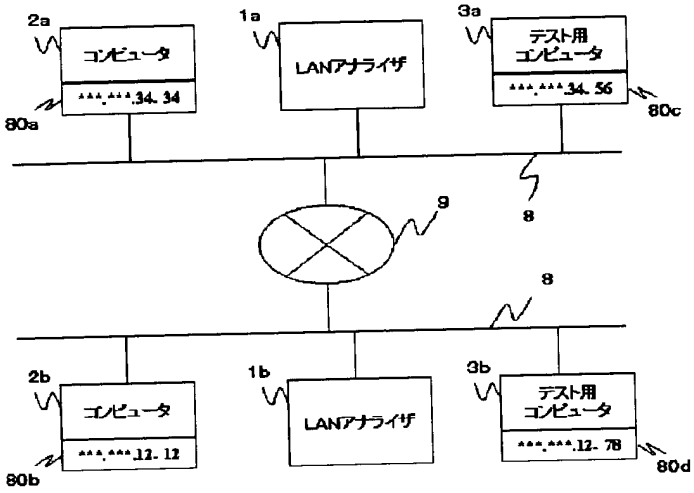
【００４１】第１の実施形態では、コンピュータ２が自らエラーを検出してテストコンピュータ３宛てのＰｉｎｇを発行した。このため、コンピュータ２がハングアップまたはダウンして、自らＰｉｎｇを発行することができないような場合は、エラーを検出することができなかった。しかし、本実施形態では、そのような場合もエラーを検出することができる。

【００４２】さらに、第１の実施形態では、コンピュータ２の内部にエラー検出部２３を設ける必要がある。しかし、現実には、コンピュータ２内部にエラー検出部を設けたくない場合もある。そのような場合に、本実施形態のような構成にすれば、コンピュータ２には手を加えることなく、監視コンピュータ５をネットワークに追加

するだけで、同様の機能を実現することができる。
【００４３】つぎに、本発明の第３の実施形態が適用されるネットワークシステムの全体構成図を図３に示す。すなわち、コンピュータ２ａ，２ｂと、ネットワーク監視装置コンピュータ６ａ、６ｂとが、ＬＡＮ８ａ，８ｂに接続されている。それぞれ同一構成のＬＡＮ８ａ，８ｂがＷＡＮ９で接続されている。ネットワーク監視コンピュータ６ａ、６ｂには、それぞれ、ＩＰアドレス８０ｅ，８０ｆが割り振られている。
【００４４】本実施形態で用いるコンピュータ２ａ，２ｂの構成は、第１の実施形態と同様である。ネットワーク監視コンピュータ６ａ、６ｂの構成を図６に示す。
【００４５】ネットワーク監視コンピュータ６は、図６に示すように、キーボード等の入力装置１０１、および、ＣＲＴ、液晶ディスプレイ等の表示装置１０２が接続されている。ネットワーク監視コンピュータ６は、通信制御部６１、データ取得部１２と、ＩＰアドレス記憶部１３と、データ判別部１４と、データ取得制御部１６と、表示制御部１８とを、その内部機能として備える。これらの内部機能は、プロセッサが所定のプログラムを読み込んで、それを実行することにより実現される。
【００４６】通信制御部６１は、ネットワーク上の他の装置との通信を制御する。例えば、ネットワーク上の他の装置へ送信するために、パケットを生成して、ＬＡＮ８へ出力する。具体的には、ネットワーク監視コンピュータ６ａであれば、データ判別部１４から通知を受けると、ＩＰアドレス記憶部１３からネットワーク監視コンピュータ６ｂのＩＰアドレス８０ｆを取得して、Ｐｉｎｇを送る。
【００４７】ＩＰアドレス記憶部１３には、自ネットワーク監視コンピュータ６に割り当てられたＩＰアドレス８０と、他のＬＡＮ８に接続されているネットワーク監視コンピュータ６に割り当てられたＩＰアドレス８０とを記憶する領域を備える。例えば、ネットワーク監視コンピュータ６ａであれば、自コンピュータ６用の領域にＩＰアドレス８０ｅ（***.***.34.78）を記憶し、他のネットワーク監視コンピュータの領域にＩＰアドレス８０ｆ（***.***.12.89）を記憶している。
【００４８】データ判別部１４は、取り込んだパケットの送信先のＩＰアドレスが、ＩＰアドレス記憶部１３の自装置用ＩＰアドレス記憶領域に記憶されているＩＰアドレスと一致するかどうかを判別する。つまり、ネットワーク監視コンピュータ６ａでは、取り込んだパケットの送信先ＩＰアドレスが、ＩＰアドレス８０ｅ（***.***.12.89）であるかどうかを判別する。判別の結果、一致する場合は、その旨を通信制御部６１およびデータ取得制御部１６へ通知する。
【００４９】本実施形態のネットワーク監視コンピュータ６には、ＩＰアドレスが割り振られているので、他の実施形態と異なり、テスト用コンピュータ３を備える必要がない。つまり、自コンピュータ６宛てのパケットを受信すると、データ保持部１２２が更新されない。これにより、自コンピュータ６宛てのパケットを取得した時点でデータ保持部１２２に記憶されているパケットが、そのまま保持される。
【００５０】さらに、ネットワーク上の他の装置に対してパケットを送出することができるので、コンピュータ２は、同一ＬＡＮ８上のネットワーク監視コンピュータ６に対してエラー検出を通知するＰｉｎｇを送ればよい。
【００５１】なお，第１の実施形態において、ＬＡＮアナライザ１とコンピュータ２を一体として構成することもできるし、第３の実施形態において、ネットワーク監視コンピュータ６とコンピュータ２を一体として構成してもよい。また、上記実施形態において説明した各構成は、可能な限り組み合わせの変更、追加、省略等をすることができる。
【００５２】さらに、上記いずれの実施形態においても、ＷＡＮ９により接続される２つのＬＡＮ８ａ，８ｂを用いて説明したが、ＬＡＮ８の数はこれ以上であっても同様である。
【００５３】
【発明の効果】本発明によれば、ネットワーク監視装置が取り込んだデータに応じて、保持しているデータの更新しないようにすることができる。
【図面の簡単な説明】
【図１】本発明が適用される第一の実施形態におけるネットワークシステムの全体構成図である。
【図２】本発明が適用される第二の実施形態におけるネットワークシステムの全体構成図である。
【図３】本発明が適用される第三の実施形態におけるネットワークシステムの全体構成図である。
【図４】（ａ）は、本発明にかかる実施形態におけるＬＡＮアナライザの構成を説明する説明図であり、（ｂ）は、本発明にかかる実施形態におけるコンピュータの構成を示す説明図である。
【図５】本発明にかかる実施形態における監視コンピュータの構成を示す説明図である。
【図６】本発明にかかる実施形態におけるネットワーク監視コンピュータの構成を示す説明図である。
【図７】本発明にかかるＬＡＮアナライザの処理手順を示すフローチャートである。
【図８】本発明にかかる監視コンピュータの処理手順を示すフローチャートである。
【符号の説明】
１…ＬＡＮアナライザ、２…コンピュータ、３…テスト用コンピュータ、５…監視コンピュータ、６…ネットワーク監視コンピュータ、８…ＬＡＮ、９…ＷＡＮ。

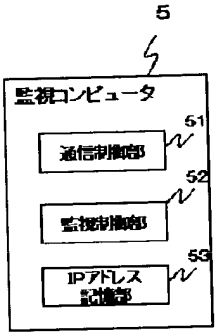
【図1】

図1



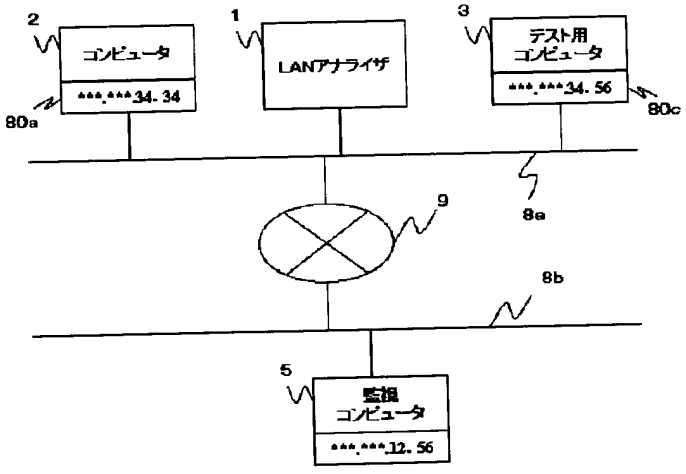
【図5】

図5



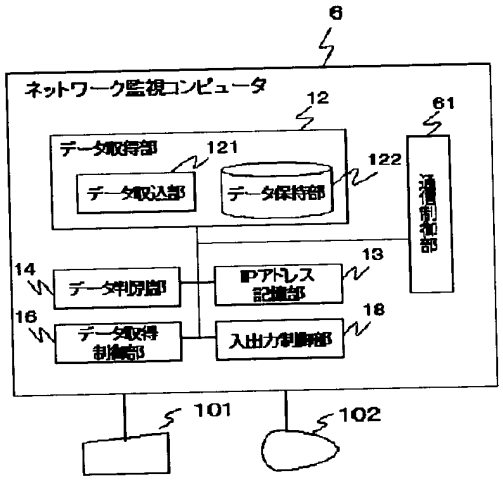
【図2】

図2



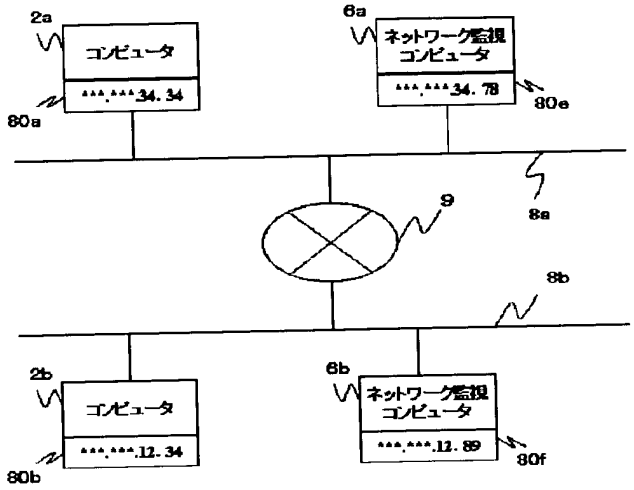
【図6】

図6



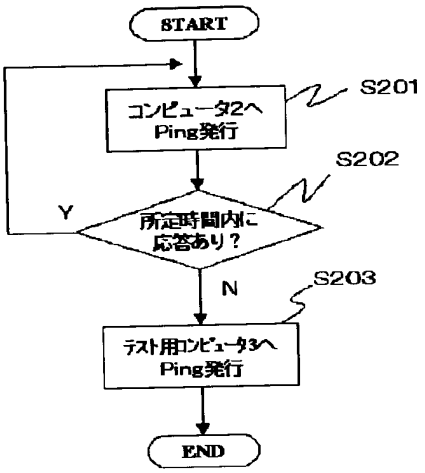
【図3】

図3



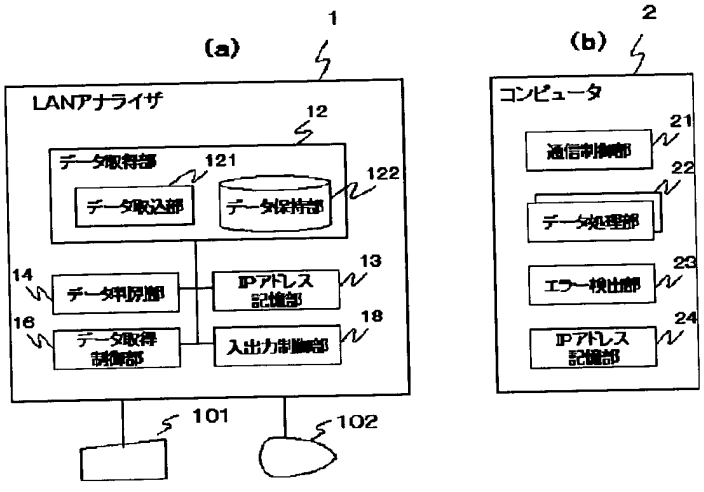
【図8】

図8



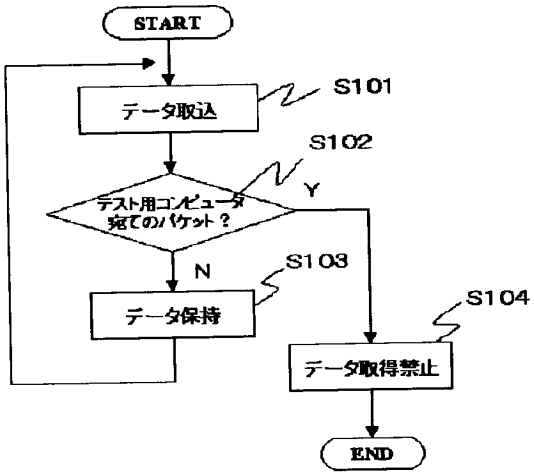
【図4】

図4



【図7】

図7



フロントページの続き

(72)発明者　山岸　令和
神奈川県横浜市戸塚区品濃町504番地２
日立電子サービス株式会社内
(72)発明者　武貞　睦治
神奈川県横浜市戸塚区品濃町504番地２
日立電子サービス株式会社内

Ｆターム(参考)　5K030 GA11 GA17 HB28 HB29 HC01
HC14 HD06 JA10 KA04 KA06
5K033 AA03 AA04 CC01 DA01 DA06
DB20 EA03
5K035 AA02 AA04 KK01